UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

JAY TAYLOR and SHELLEY TAYLOR, individually and on behalf of all others similarly situated, Plaintiffs, v. MCG HEALTH, LLC, Defendant.	No. **CLASS ACTION COMPLAINT** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiffs Jay Taylor and Shelley Taylor, individually, and on behalf of all others similarly situated, bring this action against Defendant MCG Health, LLC ("MCG Health" or "Defendant"), a Washington corporation, to obtain damages, restitution and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. Defendant is a HIPPA business associate that provides patient care guidelines to

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

health care providers and health plans.

2. As a condition of its services, Defendant requires patients and/or patient healthcare networks to provide sensitive and private information, including, but not limited to, patient names, gender, telephone numbers, addresses, dates of birth, Social Security numbers, and medical and code information.

3. On March 25, 2022, Defendant discovered an unauthorized party previously obtained certain personal information of its customers' patients and members that matched data stored on Defendant's systems (the "Data Breach"). The affected patient and/or member data included some or all of the following data elements: names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gender.

4. Upon learning of the issue, Defendant investigated the Data Breach and discovered that an unauthorized party may have acquired the Private Information of Plaintiffs and approximately 1,100,000 Class Members on or around February 25, 2022 and February 26, 2022

5. Despite discovering the Data Breach on March 10, 2022, Defendant did not notify Plaintiffs and Class Members until June 10, 2022 ("Notice of Data Breach").

6. As a result of the Data Breach, Plaintiffs and over a million Class Members suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, and the loss of, and diminution in, value of their personal information.

7. In addition, Plaintiffs' and Class Members' sensitive confidential Information—which was entrusted to Defendant—was compromised and unlawfully accessed due to the Data Breach. This information, while compromised and taken by unauthorized third parties, remains

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

also in the possession of Defendant, and without additional safeguards and independent review and oversight, remains vulnerable to additional hackers and theft.

8. Information compromised in the Data Breach includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gend**er**, and potentially other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") that Defendant collected and maintained (collectively referred the "Private Information")[1].

9. Defendant did not notify patients that their Private Information was subject to unauthorized access resulting from the Data Breach until June 10, 2022, nearly two-and-a-half months after the attack was launched and the Data Breach was discovered.

10. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patients' and employees' Private Information.

11. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party.

12. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks.

---

[1] The term "Private Information" includes separately and jointly the terms "Personally Identifiable Information" ("PII") and "Protected Health Information" ("PHI"). Specifically, Plaintiffs allege the information disclosed in the Data Breach constitutes both PII (*e.g.*, name, address, and SSN) and PHI (*e.g.*, name, SSN, gender, medical code).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

13. The mechanism of the hacking and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant and entities like it, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition and vulnerable to theft.

14. Defendant disregarded the rights of Plaintiffs and Class Members (defined below) by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiffs and Class Members prompt notice of the Data Breach.

15. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner, as opposed to letting cyberthieves roam freely in Defendant's IT network for nearly two full weeks.

16. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their respective lifetimes.

17. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

but with another person's photograph, and giving false information to police during an arrest.

18. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

19. Plaintiffs and Class Members will incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

20. Plaintiffs seek to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

21. Plaintiffs seek remedies including, but not limited to, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

22. Plaintiffs also seek injunctive and equitable relief to prevent future injury on behalf of himself and the putative Class.

PARTIES

23. Plaintiffs Jay and Shelley Taylor are, and at all times mentioned herein were, individual citizens of the Commonwealth of Kentucky residing in Mt. Sterling. Plaintiffs were patients of local hospitals networks which were affiliates of Defendant. Upon information and belief, Plaintiffs provided Private Information to the affiliates, which then provided Plaintiffs' Private Information to Defendant. Plaintiffs were notified of Defendant's Data Breach and their Private Information being compromised upon receiving a notice letter dated June 10, 2022.

24. MCG is a HIPAA business associate that provides patient care guidelines to health care providers and health plans. MCG Health, LLC is a Washington Limited Liability Company with a principal place of business at 901 5th Avenue, Suite 120, Seattle, WA 98164. MCG Health,

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

LLC's sole member is Hearst Healthcare Holding I, Inc., located 1301 Fifth Avenue, Suite 3800, WA 98101, and as such is a citizen of the state of Washington.

JURISDICTION AND VENUE

25. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiffs and at least one member of the putative Class, as defined below, are citizens of a different state than Defendant MCG, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs. For example, Plaintiffs are citizens of Kentucky and MCG's sole member is a citizen of Washington.

26. The Western District of Washington has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in Washington and this District through its headquarters, offices, parents, and affiliates.

27. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

DEFENDANT'S BUSINESS

28. Defendant is HIPPA business associate that provides patient care guidelines to health care providers and health plans with its principal place of business in Seattle, Washington. Defendant provides services on a nationwide basis.

29. Defendant requires Plaintiffs and Class Members or the healthcare networks that Plaintiffs and Class Members use to provide the following Private Information:

names, Social Security numbers, medical codes, postal addresses, telephone numbers, email

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

addresses, dates of birth and gender.

- Name;
- Social Security Number;
- Medical Code;
- Postal Address;
- Telephone Number;
- Email Address;
- Date of Birth; and
- Gender

30. Before receiving Defendant's services, Plaintiffs and Class Members and/or their healthcare providers were required to and did in fact turn over much (if not all) of the private and confidential information listed above.

31. On information and belief, Defendant provides each of its patients with a HIPAA compliant notice of its privacy practices (the "Privacy Notice") in respect to how they handle Private Information.

32. A copy of the Privacy Notice is maintained on Defendant's website, and may be found here: https://www.mcg.com/privacy-policy/.

33. Due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, Defendant recognizes privacy rights, and promises in its Privacy Notice, to, among other things, maintain the privacy of patients' protected health information, which includes the types of data compromised in this Data Breach.

34. Defendant promises to maintain the confidentiality of Plaintiffs' and Class Members' Private Information to ensure compliance with federal and state laws and regulations,

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

and not to use or disclose Plaintiffs' and Class Members' Private Information for any reasons other than those expressly listed in the Privacy Notice without written authorization.

35. As a condition of receiving Defendant's services, Defendant requires that Plaintiffs and Class Members entrust it with highly sensitive personal information.

36. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

37. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members would not have entrusted Defendant with their Private Information had they known that Defendant would fail to implement industry standard protections for that sensitive information.

38. Plaintiffs and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

THE ATTACK AND DATA BREACH

39. On March 25, 2022, Defendant identified suspicious activity in its employee email network and determined that between February 25, 2022 and February 26, 2022 an unauthorized party had access to Plaintiffs' and Class Members' Private Information stored on Defendant's systems.

40. Defendant acknowledges that "an unauthorized party previously obtained certain of your personal information that matched data stored on [Defendant's] systems. The affected patient or member data included some or all of the following data elements: names, Social

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender."[2]

41. On information and belief, the cybercriminals did in fact access Defendant's files, and exfiltrate Plaintiffs' and Class Members' Private Information during the roughly two weeks in which the cybercriminals had unfettered access to Defendant's email network.

42. On information and belief, the Private Information contained in the emails accessed by hackers was not encrypted.

43. On information and belief, the cyber-attack was targeted at Defendant due to its status as a HIPAA associated business entity that collects, creates, and maintains Private Information.

44. On information and belief, the targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients and/or members, like Plaintiffs and the Class Members.

45. While Defendant stated in notice letters sent to Plaintiffs and Class Members (as well as on its website) that it learned of the Data Breach in March 2022, Defendant did not begin notifying impacted patients, such as Plaintiffs and Class Members, until June 10, 2022– nearly two and a half months after discovering the Data Breach.

46. Due to Defendant's inadequate security measures, Plaintiffs and the Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

47. Defendant had obligations created by HIPAA, contract, industry standards,

---

[2] https://www.mcg.com/wp-content/uploads/2022/06/MCG-Website-Notice_90273447_1-6.8.22481312.4-004.pdf (last accessed June 28, 2021).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

common law, and its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

48. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

THE DATA BREACH WAS FORSEEABLE

49. Defendant's data security obligations were particularly important given the substantial increase in ransomware attacks and/or data breaches in the healthcare industry preceding the date of the breach.

50. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.3 Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.4 The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.5 These incidents continue to rise in frequency, with an estimated 1,862 data breaches occurring in 2021.[6]

51. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida

---

[3] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed June 28, 2021).
[4] *Id*.
[5] *Id* at p15.
[6] https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed June 28, 2021).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

52. In 2021 alone, there were over 220 data breach incidents.[7] These approximately 220 data breach incidents have impacted nearly 15 million individuals.[8]

53. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[9]

54. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[10]

55. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

56. As a sophisticated healthcare entity that collects and stores a particularly sensitive PII, an email phishing attack, and the potential harms arising therefrom, was reasonably foreseeable to Defendant.

---

[7] *See* Kim Delmonico, Another (!) Orthopedic Practice Reports Data Breach, Orthopedics This Week (May 24, 2021), https://ryortho.com/breaking/another-orthopedic-practice-reports-data-breach/.
[8] *Id*.
[9] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited July 2, 2021).
[10] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

DEFENDANT FAILED TO PROPERLY PROTECT PLAINTIFFS' AND CLASS MEMBERS' PRIVATE INFORMATION

57. Defendant did not use reasonably security procedures and practices appropriate to the nature of the sensitive, unencrypted Private Information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information for more than 1,100,000 individuals.

Defendant failed to properly comply with Federal Trade Commission ("FTC") data security standards

58. The FTC promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

59. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.11 The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[12]

60. The FTC further recommends that companies not maintain PII longer than is

---

[11] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 15, 2021).

[12] *Id*.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

61. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

62. These FTC enforcement actions include actions against healthcare providers like Defendant. See, e.g., *In the Matter of Labmd, Inc*., A Corp, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

63. Defendant failed to properly implement basic data security practices explained and set forth by the FTC.

64. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

65. Defendant was at all times fully aware of its obligation to protect the Private Information of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

Defendant failed to comply with industry standards

66. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information for more than 1,100,000 individuals.

67. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[13]

68. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share

[13] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[14]

69. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

[14] *Id.* at 3-4.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[15]

70. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and

[15] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Aug. 23, 2021).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

[information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[16]

71. As described above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

72. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

73. Other best cybersecurity practices that are standard in the healthcare industry

[16] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Aug. 23, 2021).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

74. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

75. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

76. Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

77. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information. And phishing is undoubtedly a well-known and common attack vector about which Defendant should have been aware and prepared to repel.

78. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Those safeguards must include physical, technical, educational, and administrative components.

79. Title II of HIPAA contains what are known as the Administrative Simplification

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

80. Given that Defendant was storing the Private Information of more than 1,100,000 individuals—and likely much more than that—Defendant could and should have implemented all of the above measures to prevent ransomware attacks.

81. The occurrence of the Data Brach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of approximately 1,100,000 individuals' Private Information.

DEFENDANT'S BREACH

Defendant failed to properly protect Plaintiffs' and Class Members' Private Information

82. Defendant breached its obligations to Plaintiffs and Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, hacking incidents, and ransomware attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing or prior intrusions;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

d. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

g. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

h. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

i. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

k. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

l. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

m. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

n. Failing to adhere to industry standards for cybersecurity.

83. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

84. Accordingly, as outlined below, Plaintiffs and Class Members now face a present, increased, and immediate risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

Cyberattacks and data breaches cause disruption and put individuals at an increased risk of fraud and identity theft

85. Hacking incidents and data breaches at healthcare related companies like Defendant are especially problematic because of the sensitive nature of the information at issue and the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

86. Researchers have found that at medical facilities that experienced a data security

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

incident, the death rate among patients increased in the months and years after the attack.[17]

87. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[18]

88. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[19]

89. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate

---

[17] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[18] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[19] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

90. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[20]

91. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

92. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

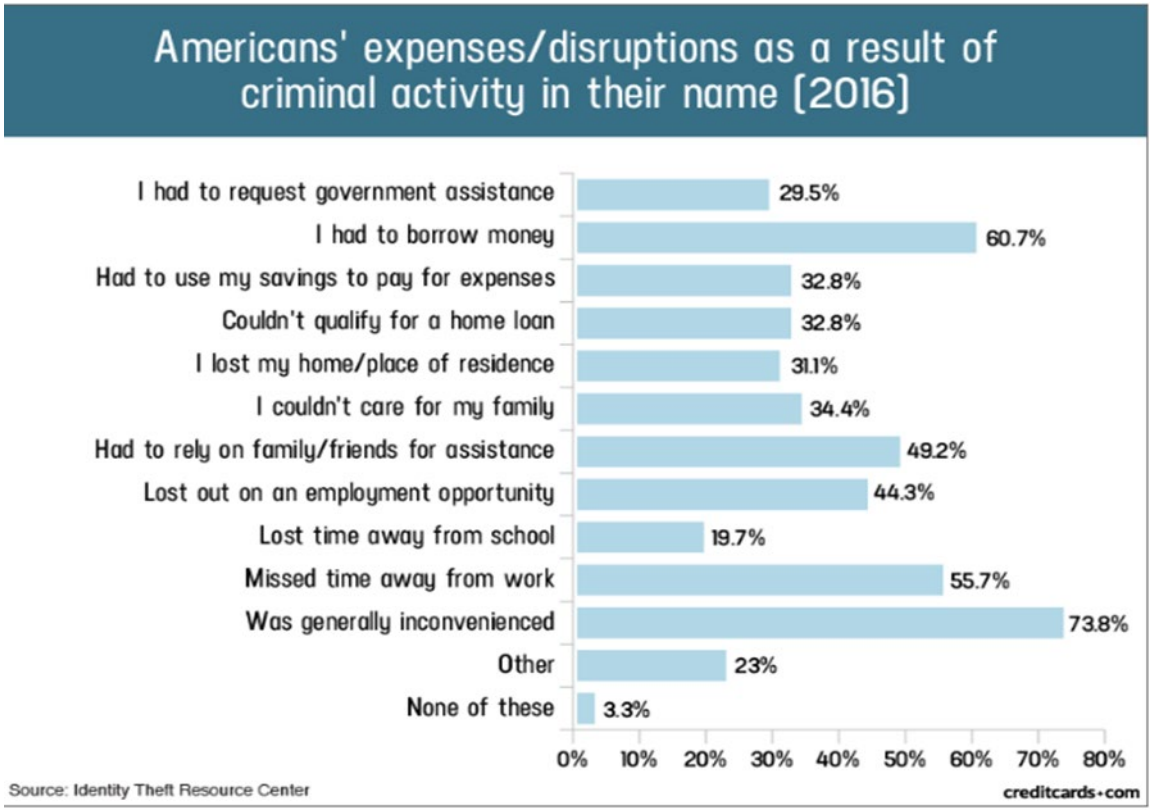
93. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[21]

---

[20] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Mar. 16, 2021).

[21] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711



94. Moreover, theft of Private Information is also gravely serious. PII and PHI are extremely valuable property rights.[22]

95. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

96. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment,

[22] See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

insurance and payment records, and credit report may be affected."[23]

97. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

98. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

99. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

100. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

101. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the

---

[23] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Mar. 16, 2021).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

future.

102. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

103. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[24] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

104. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[25] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[26] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

105. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

106. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be

---

[24] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[25] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 16, 2021).
[26] *Id* at 4.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[27]

107. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[28]

108. Medical information is especially valuable to identity thieves.

109. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[29] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[30]

110. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

111. For this reason, Defendant knew or should have known about these dangers and strengthened its network and data security systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

---

[27] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[28] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[29] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/.

[30] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

Plaintiffs' and Class Members' harms and damages

112. To date, Defendant has done little to adequately protect Plaintiffs and Class Members, or to compensate them for their injuries sustained in this data breach. Defendant's data breach notice letter completely downplays and disavows the theft of Plaintiffs' and Class Members' Private Information, when the facts demonstrate that the Private Information was accessed and exfiltrated. The complimentary fraud and identity monitoring service offered by Defendant through Experian IdentityWorks is wholly inadequate as the services are only offered for 24 months and it places the burden squarely on Plaintiffs' and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

113. Plaintiffs and Class Members have been injured and damaged by the compromise of their Private Information in the Data Breach.

114. Plaintiffs' Private Information (including without limitation their names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender) was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendant's IT network. Class Members' Private Information, as described above, was similarly compromised and is now in the hands of the same cyberthieves.

115. Plaintiffs typically take measures to protect their Private Information and is very careful about sharing their Private Information. Plaintiffs have never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

116. Plaintiffs store any documents containing their Private Information in a safe and secure location. Moreover, Plaintiffs diligently chooses unique usernames and passwords for their online accounts.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

117. To the best of their knowledge, Plaintiffs' Private Information was never compromised in any other data breach.

118. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, and similar identity theft.

119. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

120. Plaintiffs and Class Members will also incur out-of-pocket costs for protective measures such as credit monitoring fees (for any credit monitoring obtained in addition to or in lieu of the inadequate monitoring offered by Defendant), credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

121. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by the hacker and cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

122. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for.

123. Plaintiffs and Class Members have spent and will continue to spend significant

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

amounts of time monitoring their financial and medical accounts and records for misuse. Indeed, Defendant's own notice of data breach provides instructions to Plaintiffs and Class Members about all the time that they will need to spend monitor their own accounts and statements received from healthcare providers and health insurance plans.

124. Plaintiffs spent many hours over the course of several days attempting to verify the veracity of the notice of breach that he received and to monitor their financial and online accounts for evidence of fraudulent activities.

125. Plaintiffs and Class Members have suffered actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

126. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing sensitive and confidential personal, health, and/or financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

127. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

128. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

CLASS REPRESENTATION ALLEGATIONS

129. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

130. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All United States residents whose Private Information was accessed or acquired during the data breach event that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and other Class Members on or around June 10, 2022 (the "Nationwide Class").

131. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate class, defined as follows:

> All Washington residents whose Private Information was accessed or acquired during the data breach event that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and other Class Members on or around June 10, 2022 (the "Nationwide Class").

132. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives,

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

133. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendant has identified hundreds of thousands of individuals whose Private Information may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records. Defendant advised the United States Department of Health and Human Services that the Data Breach affected more than 1,100,000 individuals.

134. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the hacking incident and Data Breach;

c. Whether Defendant's data security systems prior to and during the hacking incident and Data Breach complied with applicable data security laws and regulations, *e.g.*, HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Defendant owed a duty to provide Plaintiffs and Class Members notice of this Data Breach, and whether Defendant breached that duty to provide timely notice;

j. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct was *per se* negligent;

m. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

n. Whether Defendant was unjustly enriched

o. Whether Defendant's conduct violated federal law;

p. Whether Defendant's conduct violated state law;

q. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, and/or punitive damages.

135. Common sources of evidence may also be used to demonstrate Defendant's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

prove VMMC's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

136. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach and due to Defendant's misfeasance.

137. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they has suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

138. Predominance, Fed. R. Civ. P. 23 (b)(3). Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

139. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

140. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

141. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

142. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

143. Unless a Class-wide injunction is issued, Defendant may continue in its failure to

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

144. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

145. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

146. Defendant acted on grounds that apply generally to the Class as a whole, so that Class certification and the corresponding relief sought are appropriate on a Class-wide basis.

147. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

FIRST COUNT
Violation of the Washington State Consumer Protection Act
(RCW 19.86.010 *et seq.*)
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Washington Class)

148. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

149. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

150. Defendant is a "person" as described in RWC 19.86.010(1).

151. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

people of the State of Washington.

152. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

153. In the course of conducting their business, Defendant committed "unfair or deceptive acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' Private Information, and violating the common law alleged herein in the process. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

154. Defendant also violated the CPA by failing to timely notify and concealing from Plaintiffs and Class Members regarding the unauthorized release and disclosure of their Private Information. If Plaintiffs and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their Private Information, medical information, and identities.

155. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendant's wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

capacity to injure other persons.

156. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

157. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiffs and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which he or she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of his or her Private Information; (5) deprivation of the value of his or her Private Information, for which there is a well-established national and international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

158. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Private Information entrusted to it.

159. Plaintiffs, on behalf of Plaintiffs and the Class Members, also seeks to recover

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiffs, on behalf of Plaintiffs and the Class Members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each class member by three times the actual damages sustained not to exceed $25,000.00 per class member.

SECOND COUNT
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

160. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

161. Plaintiffs bring this claim individually and on behalf of the Class members.

162. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

163. Defendant had, and continues to have, a duty to timely disclose that Plaintiffs' and Class Members' Private Information within their possession was compromised and precisely the type(s) of information that were compromised.

164. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Private Information.

165. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like HIPPA and Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

Private Information.

166. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

167. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

168. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

169. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

170. Defendant systematically failed to provide adequate security for data in its possession.

171. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

a. Upon information and belief, mishandling emails, so as to allow for unauthorized person(s) to access Plaintiffs' and Class Members' Private Information;

b. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

c. Failing to adequately monitor the security of their networks and systems;

d. Failure to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards.

172. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Defendant's possession.

173. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' Private Information.

174. Defendant, through its actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiffs and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

175. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs and Class Members' Private Information would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

176. It was foreseeable that the failure to adequately safeguard Plaintiffs and Class Members' Private Information would result in injuries to Plaintiffs and Class Members.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

177. Defendant's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised.

178. As a result of Defendant's ongoing failure to notify Plaintiffs and Class Members regarding what type of Private Information has been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

179. Defendant's breaches of duty caused Plaintiffs and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

180. As a result of Defendant's negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

181. Plaintiffs seek the award of actual damages on behalf of the Class.

182. In failing to secure Plaintiffs' and Class Members' Private Information and promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiffs' and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of himself and the Class.

183. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling Defendant to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

THIRD COUNT
Negligence *per se*

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

(On Behalf of Plaintiffs and the Nationwide Class)

184. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

185. Pursuant to Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

186. Plaintiffs and Class Members are within the class of persons that the FTCA was intended to protect.

187. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

188. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

189. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

190. Plaintiffs and Class Members are within the class of persons that the HIPAA was intended to protect.

191. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

Rights ("OCR") has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiffs and the Class.

192. Defendant breached their duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

193. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

194. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

195. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure and compromise of their Private Information.

196. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, and consequential in an amount to be proven at trial.

FOURTH COUNT
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

197. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

198. Defendant provided Plaintiffs and Class Members with an implied contract to protect and keep Defendant's patients' private, nonpublic personal, financial and health information when they gathered the information from each of their patients.

199. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

200. Defendant's agreement to reasonably protect such information included compliance with healthcare industry data security standards, and with applicable data security standards that govern healthcare entities like Defendant, including HIPAA.

201. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

202. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

203. HIPAA requires covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

204. HIPAA covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

205. Healthcare industry standards for data security include several best practices that have been identified that a minimum should be implemented by healthcare providers like Defendant. These include, but are not limited to: educating all employees; strong passwords;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

206. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

207. Class Members who paid money to Defendant, or who had money paid on their behalf to Defendant, reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security that complied with healthcare industry data security standards and applicable regulations like HIPAA. Defendant failed to do so.

208. Plaintiffs and Class Members would not have provided their personal, financial or health information to Defendant, but for Defendant's implied promises to safeguard and protect Defendant's patients' private personal, financial, and health information.

209. Plaintiffs and Class Members performed their obligations under the implied contract when they provided their private personal, financial, and health information as a patient and when they paid for the services provided by Defendant.

210. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to protect and keep private the nonpublic personal, financial, and health information provided to them about Plaintiffs and Class Members.

211. As a direct and proximate result of Defendant's breach of their implied contracts, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer,

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

damages and injuries.

FIFTH COUNT
Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and the Nationwide Class)

212. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

213. As a condition of status as a person whose Private Information in Defendant's possession, Plaintiffs and the Class Member provided their Private Information. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class Members if their data had been breached and compromised or stolen.

214. Defendant offered to provide goods and services to Plaintiffs and Class Members in exchange for payment. Defendant also required Plaintiffs and Class Members to provide Defendant with their Private Information to receive services.

215. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

216. Had Plaintiffs and Class Members known that Defendant would not adequately protect their PII, Plaintiffs and members of the Class would not have entrusted Defendant with their PII.

217. Defendant represented to Plaintiffs and Class Members and/or the healthcare networks of Plaintiffs and Class Members, implicitly and otherwise, that their PII would be secure. Plaintiffs and members of the proposed Class relied on such representations when they

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

agreed to provide their Private Information to Defendant. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant without such agreement with Defendant.

218. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

219. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

220. Defendant failed to advise Plaintiffs and Class Members of the Data Breach promptly and sufficiently.

221. Defendant's duty to safeguard Plaintiffs' and Class Member's Private Information is inherent in and consistent with the contracts entered into by Defendant and Plaintiffs and Class Members.

222. Defendant would not have suffered harm by enacting industry standard measures to safeguard Plaintiffs' and Class Member's Private Information.

223. Defendant's failure to enact reasonable safeguards to protect the Private Information it collected resulted in harm to Plaintiffs and Class Members and violated the covenant of good faith and fair dealing. Similarly, Defendant's failure to timely discover the

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

breach, to timely notify affected persons, and to fully detail the scope of the breach in the "Notice of Data Security Incident," each suffices to demonstrate a breach of the covenant.

224. Plaintiffs and Class Members have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

225. Plaintiffs, on behalf of Plaintiffs and the Class, seeks compensatory damages for breach of implied contract of good faith and fair dealing, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs in addition to all other damages or relief allowed by law.

SIXTH COUNT
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class)

226. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

227. At all times during Plaintiffs' and the Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and the Class Members' Private Information that Plaintiffs and the Class provided to Defendant.

228. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and the Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

229. Plaintiffs and Class Members provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

230. Plaintiffs and Class Members also provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

231. Defendant voluntarily received in confidence Plaintiffs' and the Class Members' Private Information with the understanding that Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

232. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and the Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and the Class Members' confidence, and without their express permission.

233. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

234. But for Defendant's disclosure of Plaintiffs' and the Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and the Class Members' Private Information as well as the resulting damages.

235. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and the Class Members' Private Information. Defendant knew or should have known its methods of accepting and securing Plaintiffs' and the Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and the Class Members' Private Information.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

236. As a direct and proximate result of Defendant's breach of its confidence with Plaintiffs and the Class, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of current and former patients and their beneficiaries and dependents; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

237. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SEVENTH COUNT
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

238. Plaintiffs repeat and re-allege each and every factual allegation contained in all

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

previous paragraphs as if fully set forth herein.

239. This count is plead in the alternative to the breach of contract counts above.

240. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

241. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

242. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing also provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

243. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

244. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase their own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

decision to prioritize its own profits over the requisite security.

245. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

246. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

247. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

248. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

249. Plaintiffs and Class Members have no adequate remedy at law.

250. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

251. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

252. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

EIGHTH COUNT
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Nationwide Class)

253. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

254. In light of the special relationships between Defendant and Plaintiffs and Class Members, whereby Defendant became guardians of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members: (i) for the safeguarding of Plaintiffs' and Class Members' Private Information; (ii) to timely notify Plaintiffs and Class Members of a data breach and disclosure; and (iii) maintain complete and accurate records of what Private Information (and where) Defendant did and does

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

store.

255. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its patients' relationship, in particular, to keep secure the Private Information of its patients.

256. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

257. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

258. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

259. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

260. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

261. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

262. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

263. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

264. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

265. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

266. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized person(s) in violation of 45 C.F.R. § 164.502, et seq.

267. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

268. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

269. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

270. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs sand Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

271. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of herself and all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action and appointing Plaintiffs and Plaintiffs' counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

F. Ordering Defendant to disseminate individualized notice of the Data Breach to all Class Members;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all claims so triable.

DATED this 1st day of July, 2022.

Respectfully Submitted,

/s/ Timothy W. Emery
/s/ Patrick B. Reddy

TIMOTHY W. EMERY
WSBA No. 34078
PATRICK B. REDDY
WSBA No. 34092
EMERY REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
Phone: (206) 442-9106
Fax: (206) 441-9711
Email: emeryt@emeryreddy.com
Email: reddyp@emeryreddy.com

M. ANDERSON BERRY*
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Phone: (916) 239-4778
Fax: (916) 924-1829
Email: aberry@justice4you.com

**pro hac vice application forthcoming*

Attorneys for Plaintiffs and the Proposed Class